Revenue Cycle Advisor
powered by HCPro
ComplyAssistant

# Approaching leadership about the HITECH Act amendment

March 8, 2021 l Briefings on HIPAA

It's the age-old tale in healthcare: Your organization needs more resources, but leadership simply isn't interested in helping out.

"This has been a challenge since the pre-HIPAA days," says **Kate Borten, CISSP, CISM, HCISPP,** founder of The Marblehead Group in Marblehead, Massachusetts. "It's always been a challenge."

There is a bit of good news, however. The recent HITECH Act amendment, signed into law by former President Donald Trump on January 5, provides security officers with a "golden opportunity" to earn much-needed support from leadership, says **Rick Ensenbach, CISSP-ISSMP, CISA, CISM, CCSFP-CHQP,** Director at Wipffli LLP in Eau Claire, Wisconsin.

The amendment states that covered entities that implement a recognized security framework—as defined by National Institute of Standards and Technology Act (NIST), the Cybersecurity Act of 2015, and other programs and processes—and maintain the framework for a 12-month period may experience mitigated fines and early/favorable termination of audits from OCR.

In other words, organizations can view this as incentive to adopt specific security frameworks. Perhaps it's a headline that will grab the attention of senior leadership.

Security o!cers should take this opportunity to approach leadership and inform them about the amendment, but they should be careful in how they do so, says Ensenbach.

"They don't want to be running into leadership's office just waving this law saying, 'We've got to do this now!' " Ensenbach says. "That's typically why a lot of leadership doesn't pay attention, because they're too used to hearing the sky is falling, whether it be from IT or security or whomever."

Ensenbach recommends sitting down with leadership, explaining the law, and outlining the benefits of a more sophisticated security program. If leadership believes the organization's existing security program is adequate, it's up to the security o!cer to explain how the framework outlined by NIST or the Cybersecurity Act of 2015 could position the organization for reduced penalties should it suffer an attack.

"I would say nine out of 10 people that I run into, especially in small organizations, they want to do the right thing," Ensenbach says. "I hear it all the time—'I just can't get leadership to listen to me.' They don't feel like they're going to be a target. They don't think it's going to happen to them. They feel like it's a lot of extra money thrown into something that doesn't need to be thrown at."

The truth is, everyone is a target today. Cyberattacks against healthcare organizations have skyrocketed, and they continue to rise as patient information and financial information is handled remotely and healthcare organizations are stretched thin due to the toll of the novel coronavirus (COVID-19) pandemic.

Organizations of all sizes are falling victim to cyberattacks. The more attention the breaches receive in the media, the more likely it is that leadership in healthcare organizations will take a closer look at their own security policies. This is especially true when reports of cyberattacks are accompanied by high-alert bulletins from federal agencies such as the Cybersecurity Infrastructure and Security Agency, the FBI, and HHS, as was the case in October 2020.

"That is the kind of front-page news that gets the attention of a CEO, a president, and the board of directors," says Borten. "That can bring visibility and more budget support, more resources to the entire security program, not just to thwart the threat of ransomware, but awareness and support for all the other aspects of security, such a broad and complex field."

Like Ensenbach, Borten urges security officers to contact those in decision-making positions and leverage the potential benefits of the HITECH Act amendment.

**Gerry Blass**, president and CEO of ComplyAssistant in Colts Neck, New Jersey, says the amendment should be discussed at an oversight committee meeting within the organization. The goal is to facilitate multidisciplinary understanding and buy-in from all levels.

**Donna Grindle**, CHPC, founder and CEO of Kardon in Tucker, Georgia, has put on webinars for some of her clients and fielded questions about how security o!cers should approach leadership and explain the impact of the law.

"Everybody that I've spoken to sees this as an opportunity to kind of shake some things loose, instead of the fear factor that cybersecurity usually comes to the table with," Grindle says.